Buckinghamshire&Surrey trading standards

The Essential Guide to Online Safety

This is serious

ONS:
"There were **4.1 million** reported offences of fraud in 2024.
A **33% increase** from 2023"

The National Crime Agency:
"...we estimate only **14%** of fraud cases are being reported"

National Audit Office:
"Online fraud is now the most commonly experienced crime... it has been overlooked by law enforcement..."

Action Fraud:
"**80%** of all fraud is on the internet"

Action Fraud:
"Surrey & Sussex Police were sent **5600 reports** of fraud in 2023.
This resulted in **259** prosecutions" **(4.6%)**

FOI requests to the police revealed:
Surrey: **2357 officers** employed. **11** are on the 'Fraud Desk' (**<0.5%)**
Metropolitan: **34,328** officers employed. **245** are on the 'Fraud Desk' (**0.7%)**

House of Commons Justice Committee:
"**2 per cent** of police funding is dedicated to combating fraud but it makes up **40 per cent of reported crimes**".

Passwords

Password strength:

LondoN2018 19Evelyn82

Mix of lower & upper case and a few numbers

Barely adequate but are easy to remember

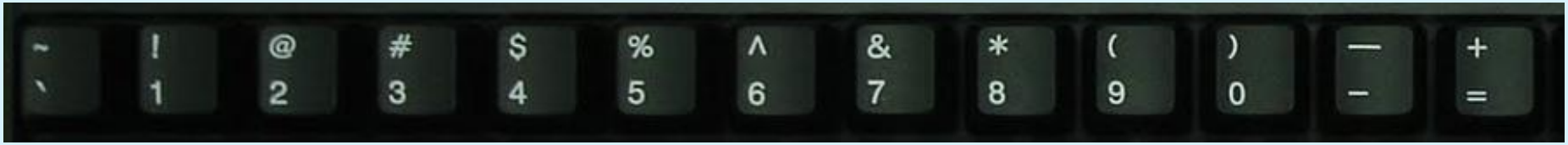
Tp4Z$rT5q1i9s&3z5c2iD

Great password but difficult to remember!

Passwords

Better passwords:

Use ‘odd’ characters from the keyboard –



These improve password strength

Passwords

Good to use different passwords for different places – but difficult to remember them all

Use a few passwords

Use more complex passwords for important websites

(Websites that don't store your personal details could all have the same password. Examples - BBC, newspapers, e-card sites, DIY stores etc)

The National Cyber Security Centre recommend you do **NOT** change your password regularly

(But do change it if you think it's been compromised)

Passwords

Good Passwords – that you can remember:

Use an acronym that means something to you.

My daughter's birth date is 13 April 1982

Can become: **Md'sbd13Apr82**

or

Use three random words

Example:

Fruitbowl.Wardrobe.Printer

Passwords

Don’t use:

Something that you might refer to in a conversation
(Partners / child’s / grandchild’s name, favourite sports team,
street where you live, pet’s name etc)

Do use:

Something that doesn’t come up in conversation:
(Mother’s place of birth, partner’s middle name, father’s first name etc)

Consider:

A Password Manager -‘ProtonPass’ ‘Nordpass’ ‘1Password’ etc
(Search for ‘password manager’)

Passwords

Don’t forget your mobile phone!

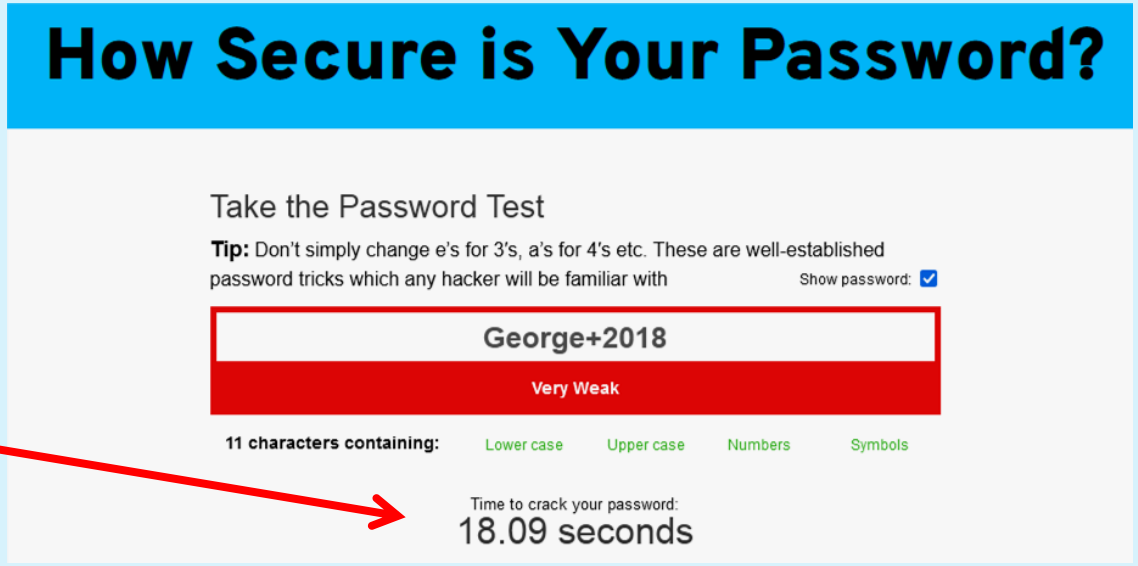
Most are purchased with no password set

(Use fingerprint / facial recognition if available)

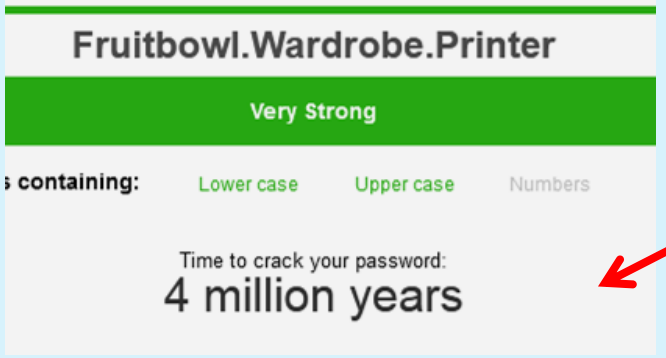
Passwords

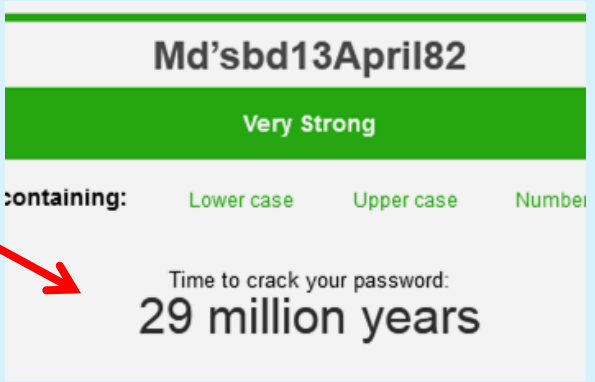
Whatever password you choose, find out how good it is at **passwordmonster.com**

A password based on your grandson's name and birth year doesn't take long to break



These passwords take a bit longer





Passwords – a final word

Two Step Authorisation (2SA)
Also known as **Two Factor Authorisation** (2FA)

Adds a second layer of security –
in addition to your password

The website sends a code - usually via text - that you have to enter before you can finish signing in.

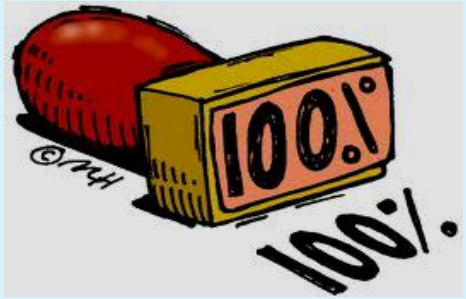
If it's an option – enable it

Bank Accounts

Secure Banking Promise

You can reclaim any money lost as long as you haven't displayed "Gross negligence"

Bank security is probably perfect



So – scammers try to trick *you* into giving them your details

Phishing

Maybe like this:

PayPal

Because it has expired, your credit card has been removed from your PayPal account.

If this was the only credit card on your PayPal account, you will need to add a new card to continue sending instant PayPal payments.

To add a new debit or credit card, log in to your PayPal account at www.paypal.co.uk, go to your Profile, and click **My money**.
Yours sincerely,
PayPal Direct

If you clicked on the link...

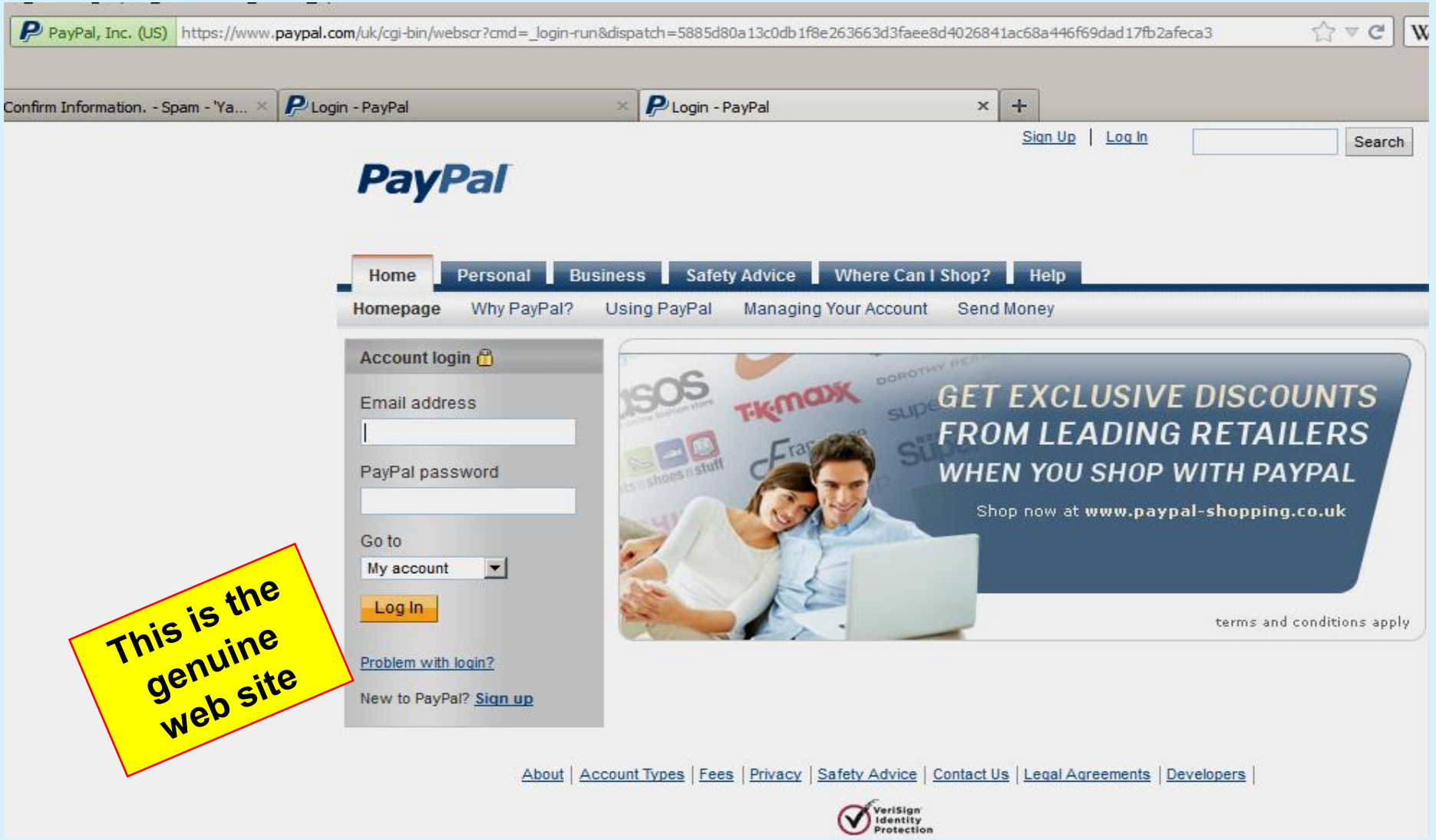
Phishing

You'd arrive here...

Looks good, but this is a web forgery

But you thought you were here

Phishing



This is the genuine web site

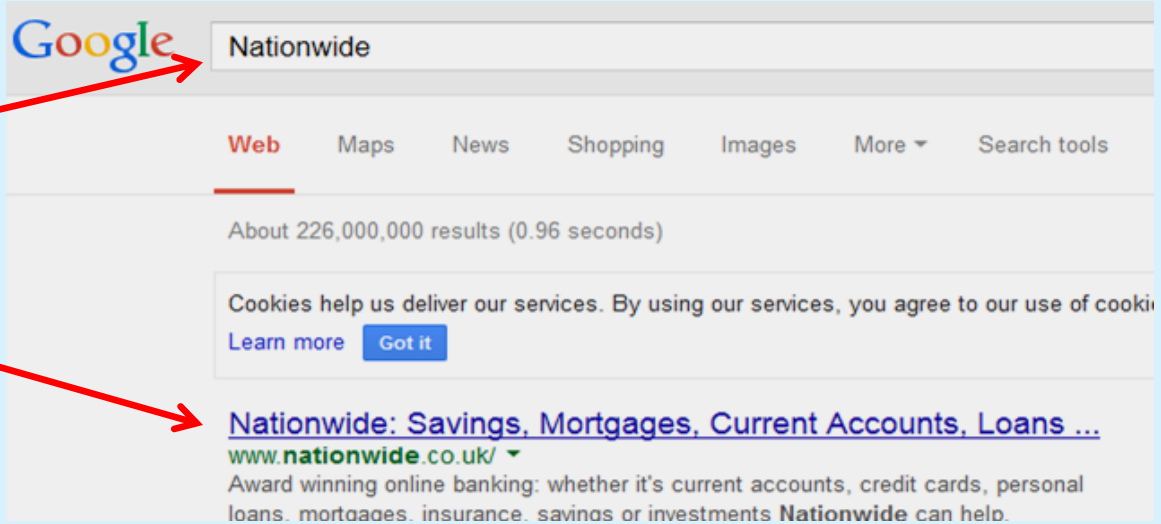
Phishing

Look at the real website address

It is safest to type in the web address yourself

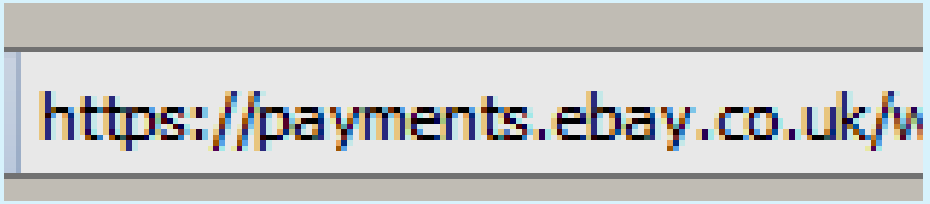
Or carry out your own web-search...

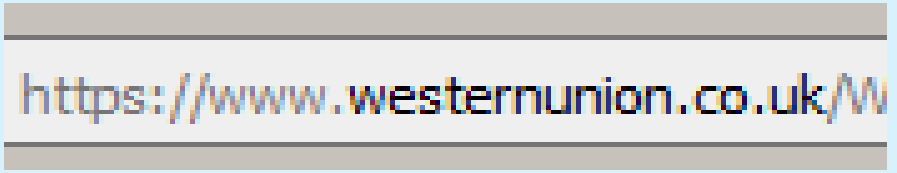
and follow the link



Using Money Online

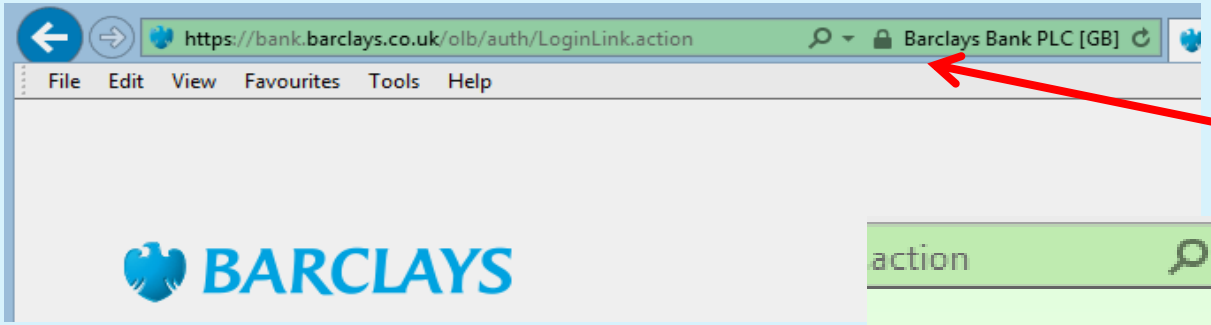
Http**s** means your data cannot be intercepted. But it doesn't mean it is a **trustworthy** site





The small padlock is <u>not</u> a guarantee that the site is trustworthy

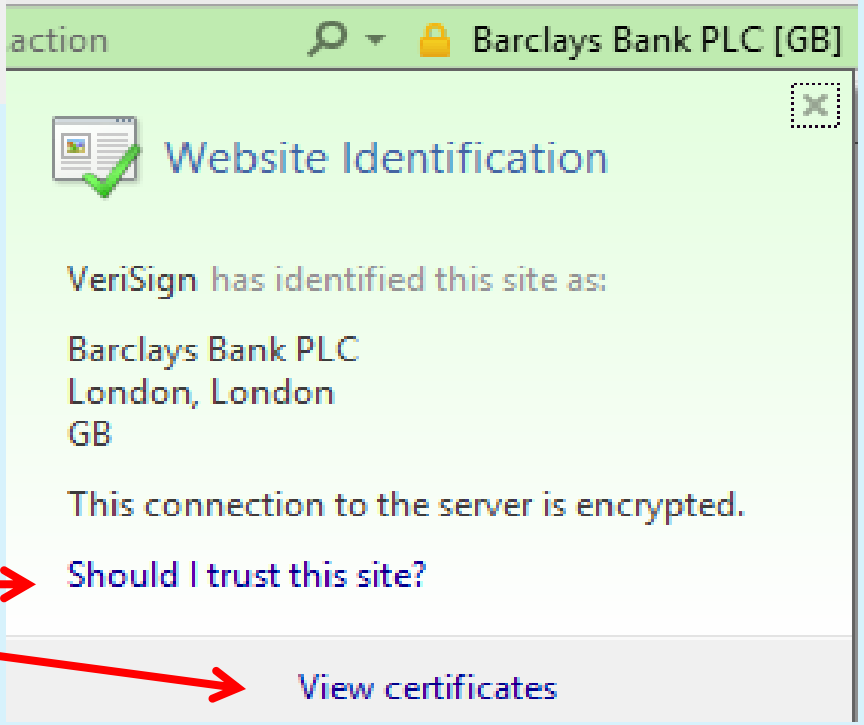
Using Money Online



Click on the padlock....

You will see more information – check the details

And follow the links for more detailed information



It should give you confidence that it is a genuine site

Using Money Online

Use a credit card instead if you can.
The seller won't know your bank details and the card company will have a method of dispute resolution

For an extra layer of security:

Sign up to an online payment platform:
PayPal / Apple Pay / Google Pay

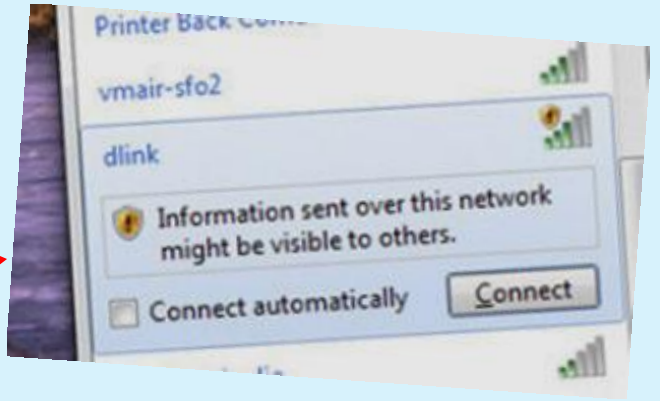
It puts a trustworthy agent between you and the supplier

They all have a dispute resolution centre

Use it to pay the supplier, if it's an option

Public Wifi

Public internet access is inherently unsafe



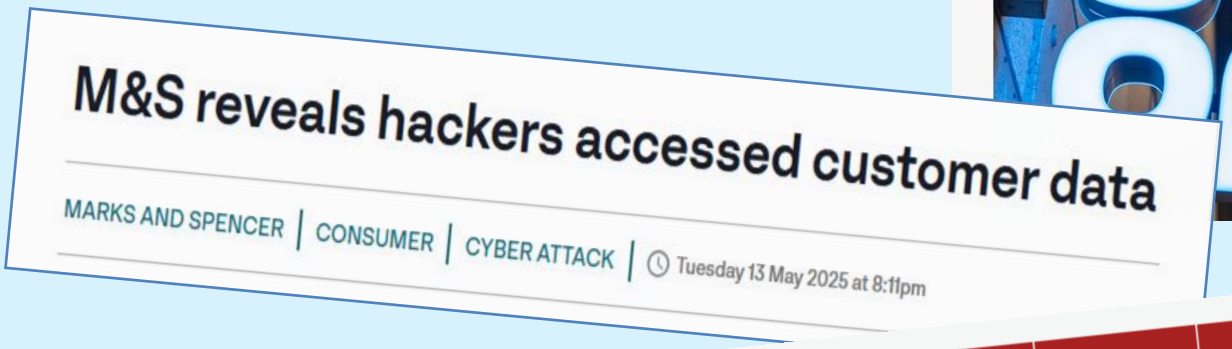
A hacker can access your device if they are using the same router

If you use public WiFi, **never** do anything confidential or use a debit or credit card

Safer Internet Browsing

We've all heard of service providers being hacked

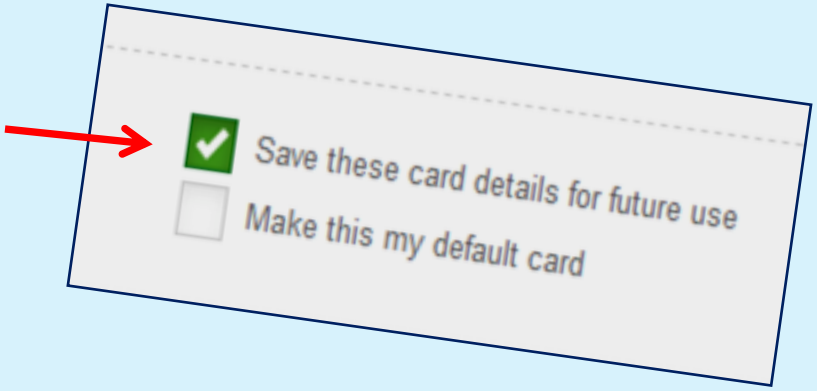
Maybe your data was stolen...

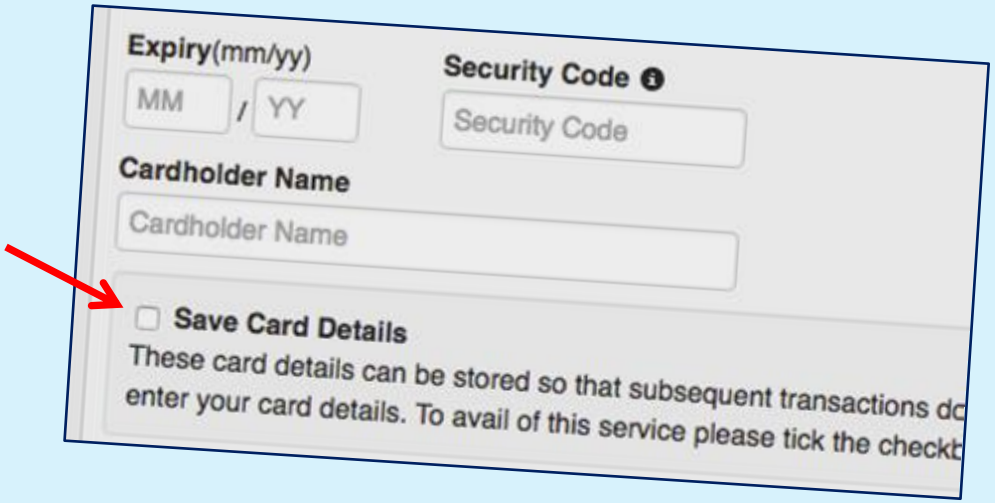


Safer Internet Browsing

It is not quite as convenient, But if you **don't** allow the provider to store your card details, you'll be less exposed

Make sure the 'Save' box is not ticked





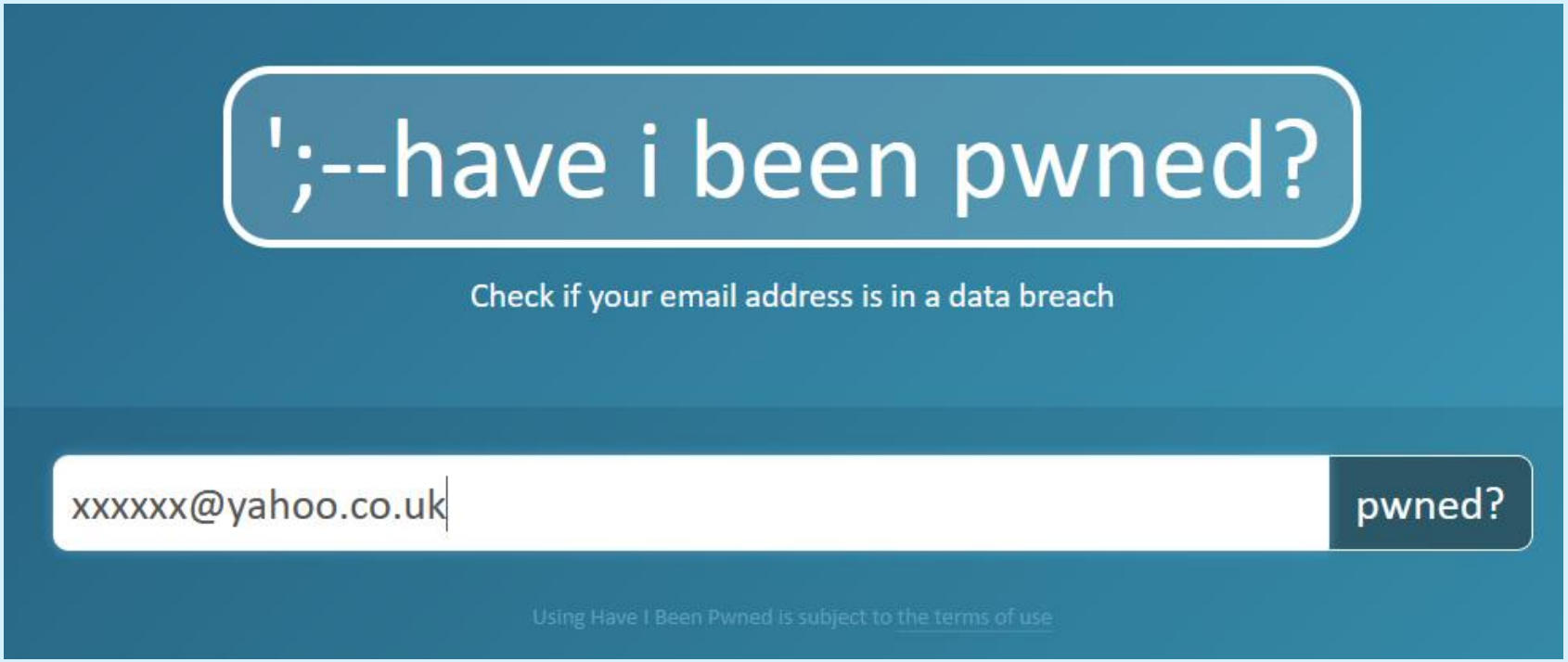
After a data breach, be **very** suspicious of any emails asking you to 'confirm your details' or reset your password

Has your data been stolen?

Visit

haveibeenpwned.com

Enter your email address into the box and click on ‘pwned?’



Has your data been stolen?

haveibeenpwned.com

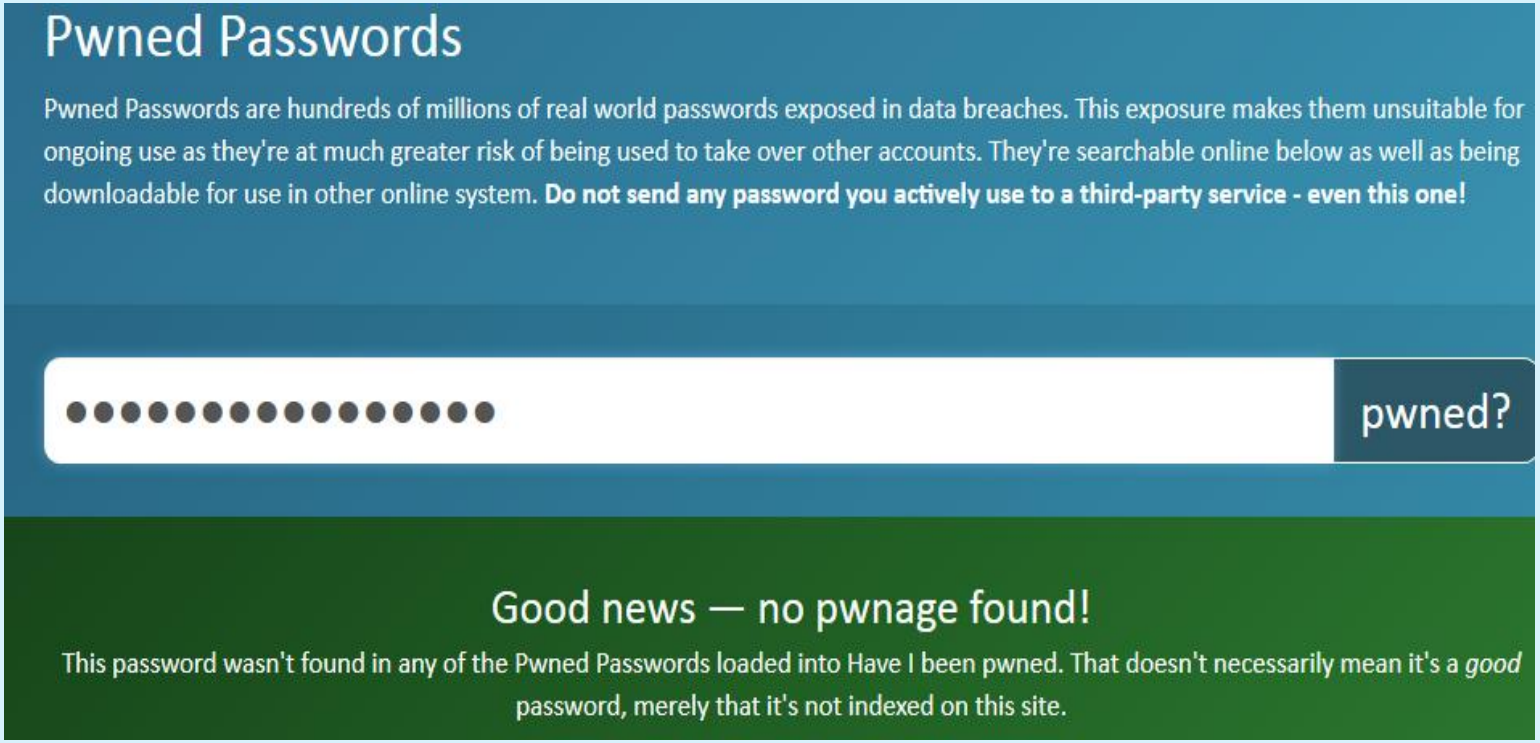
If you see this message -

You need to change the password on that account

Has your data been stolen?

haveibeenpwned.com

On the same site, you can see if **any** password you use has been found on a compromised site



This does not measure the strength of a password
Just if it's been found in a data breach

Email Scams

Scam emails are better than they were

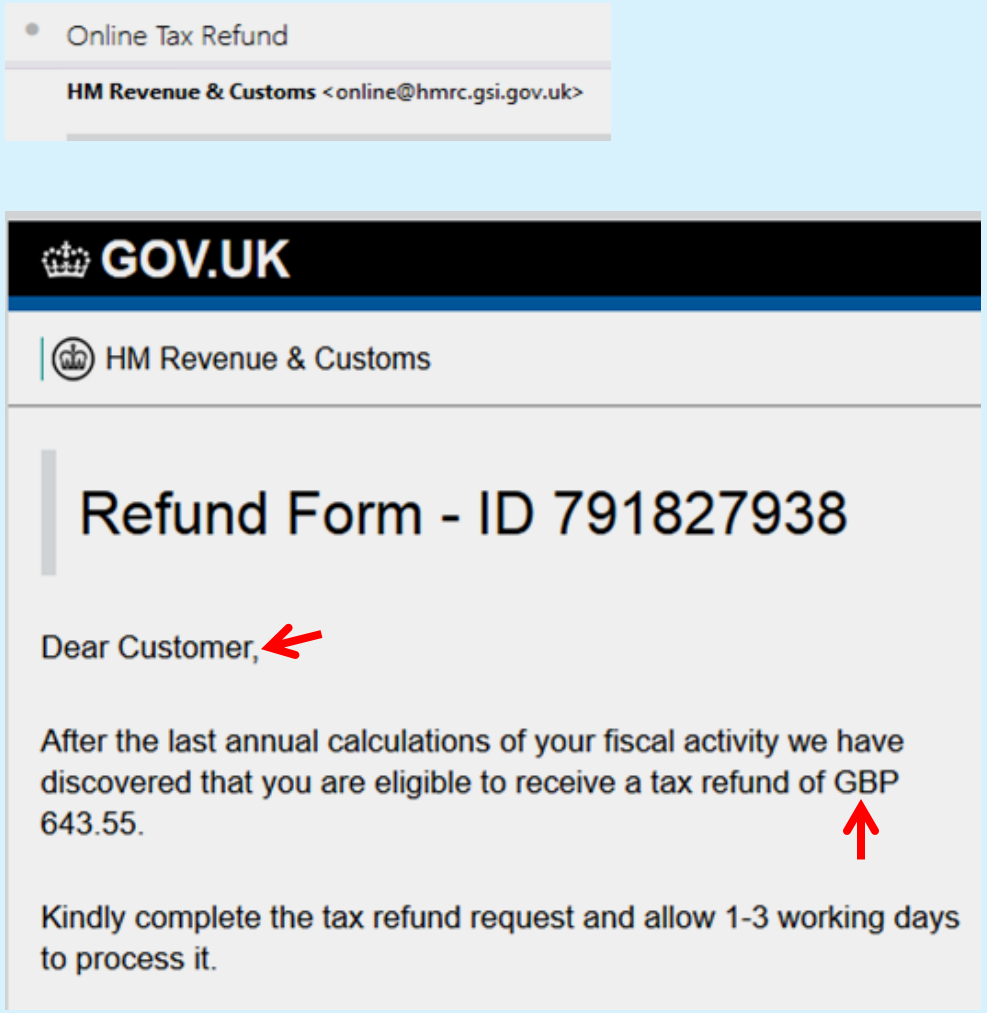
It has a genuine looking email address

Correct logo

No spelling or grammar mistakes

A believable £643.55

BUT: Not addressed to you and no '£' sign



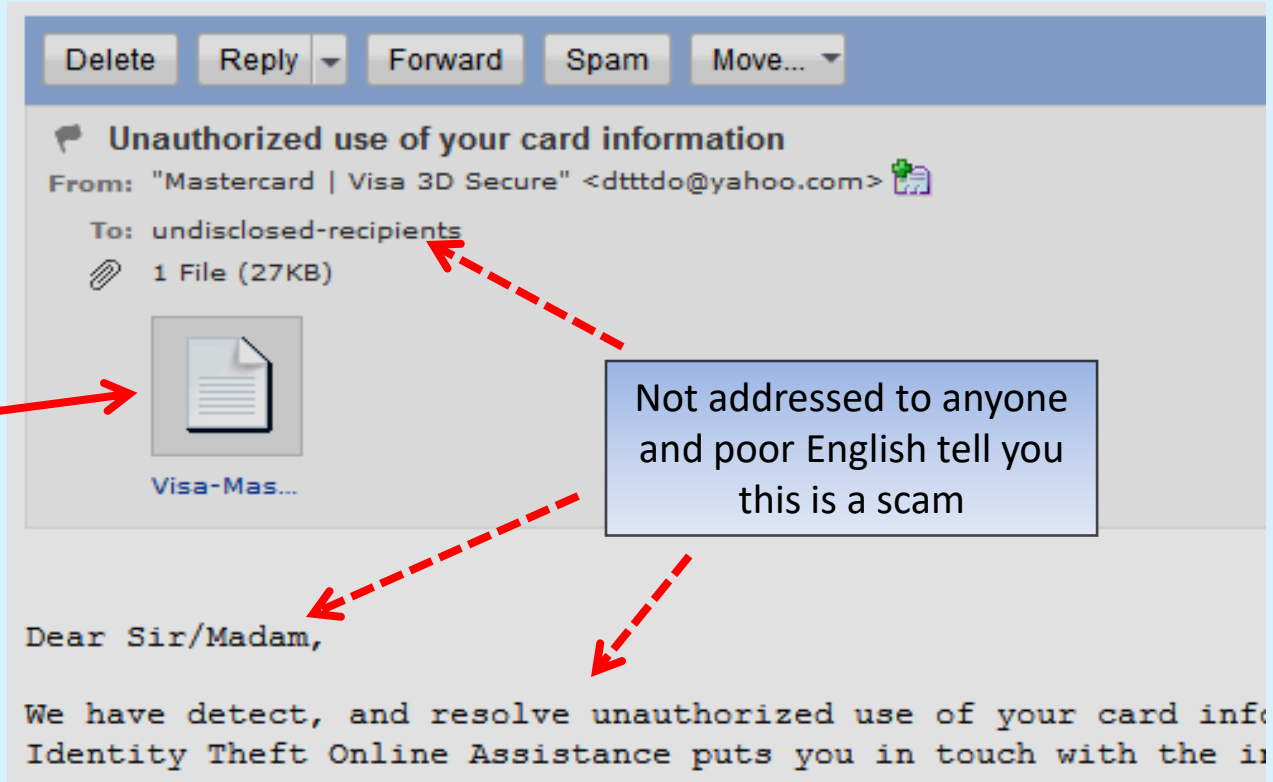
Email Scams

Forward this to report@phishing.gov.uk and the National Cyber Security Centre (ncsc.gov.uk) will try to get the sender shut down

Then click on 'Spam'. This email will be sent to your Spam folder

All future emails from this address will bypass your 'In' box and sent straight to the spam folder

A suspicious attachment. Don't click on it



And...

Never reply or 'unsubscribe' as you just confirm your email address is active

Email is Not Secure

Why does your bank never email statements to you?

Because email is <u>not</u> secure

https://mail.google.com/

https://mail.yahoo.com/

Google have said they have (now) stopped reading emails for keywords to show more personalised adverts

You might log-on to an http**<u>s</u>** website, but the email will be forwarded on to many computers during it's journey

It *travels in plain text* over the network and will be *stored in plain text* on email servers

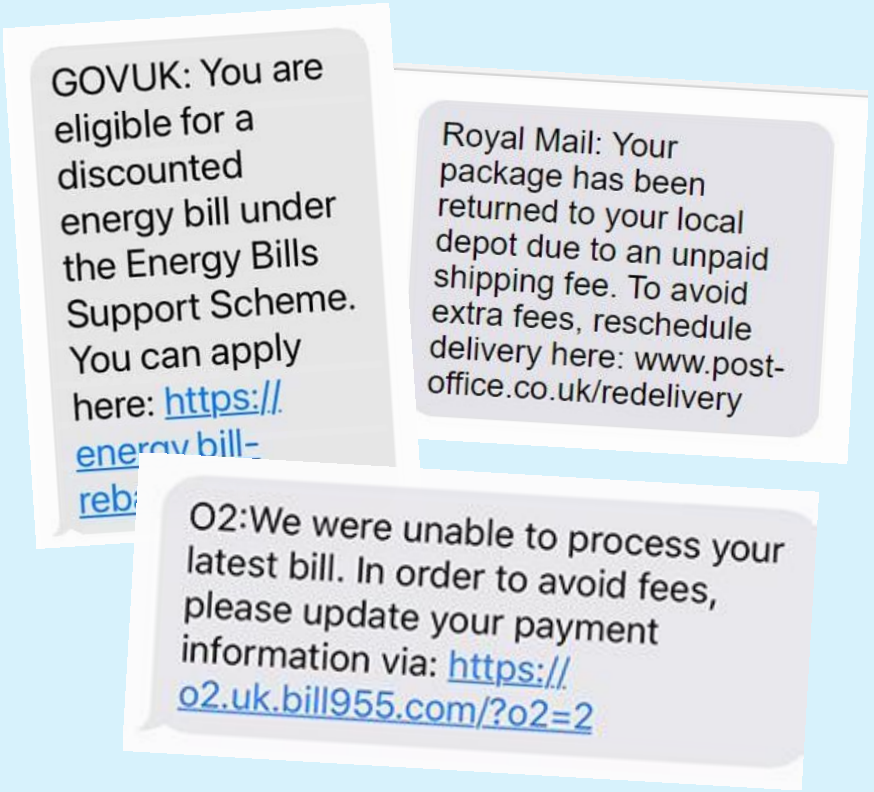
Think of your email as a postcard!

For a secure email, search for: Proton Mail, Startmail, Tutanota, Zohomail or Thexyz

Text & Phone Scams

If you receive a phishing / scam text, NEVER respond.
Forward them **7726** and the National Cyber Security Centre will get the sender shut down.

(**7726** spells SPAM on an alphanumeric keypad)



If you receive a phone call claiming to be from your bank or building society, hang up and phone **159**

https://stopscamsuk.org.uk/159

Social Media Safety

Use extra precautions when using social media on mobile devices

According to the Surrey Police...

Don't:

Tweet photos from inside your home

Mention your address on any social network

Announce when you're going on holiday

Post your holiday pictures whilst on holiday

Post photos of new expensive items you've bought or received

Assume the safety settings of your social profiles are where you left them

The Essential Guide to On-line Safety

welivesecurity™

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

For further study, the following websites are recommended:

actionfraud.police.uk
cyberaware.gov.uk
getsafeonline.org
thinkuknow.co.uk
thinkjessica.com
bbc.co.uk/webwise
welivesecurity.com
takefive-stopfraud.org.uk
ncsc.gov.uk
disney.co.uk/internet-safety

Don't forget your bank or building society will have their own security pages!

The Essential Guide to Online Safety – the last slide!

I hope this presentation has been useful

A pdf version of these slides is available at

https://tinyurl.com/5bmm6x5z

Or use:

Any feedback (good or bad) is gratefully received at:

presentationfeedback2023@gmail.com

Thank you in advance!